3.1 Der Pseudoprimzahltest

Woran erkennt man, dass eine Zahl prim ist? Der „naive“ Ansatz, Probedivisionen durch alle Zahle $\leq \sqrt{n}$ durchzuführen – perfektioniert im Sieb des ERATOSTHENES –, ist nicht effizient, da $\sqrt{n} = \exp(\frac{1}{2}\log n)$ immer noch exponentiell mit der Stellenzahl $\log n$ von n wächst.

Einen Ansatz, Primzahlen ohne Probedivision zu erkennen, bietet der Satz von FERMAT: Ist n prim, so $a^{n-1} \equiv 1 \pmod{n}$ für alle $a = 1, \ldots, n-1$. Umgekehrt sagt man, dass n den **Pseudoprimzahltest zur Basis** a besteht, wenn $a^{n-1} \equiv 1 \pmod{n}$. Eine Primzahl besteht diesen Test also zu jeder Basis $a = 1, \ldots, n-1$. Die Kongruenz $2^{14} \equiv 4 \pmod{15}$ beweist, dass 15 nicht prim ist. Allerdings ist $2^{340} \equiv 1 \pmod{341}$, obwohl $341 = 11 \cdot 31$; aber immerhin ist $3^{340} \equiv 56 \pmod{341}$, so dass 341 durch den Pseudoprimzahltest zur Basis 3 fällt.

Trotzdem reicht dieses Kriterium nicht, um umgekehrt die Primzahleigenschaft zu beweisen. Man nennt n CARMICHAEL**-Zahl**, wenn n den Pseudoprimzahltest zu jeder zu n teilerfremden Basis a besteht, aber nicht prim ist.

Den Pseudoprimzahltest kann man auch dadurch ausdrücken, dass die Ordnung von a in $\mathbb{M}_n$ ein Teiler von $n-1$ ist. Also ist n genau dann CARMICHAEL-Zahl oder prim, wenn $\lambda(n) \mid n-1$ für die CARMICHAEL-Funktion λ. Es gibt zu viele CARMICHAEL-Zahlen, als dass der Pseudoprimzahltest ruhigen Gewissens als für die Praxis ausreichend betrachtet werden könnte. Insbesondere haben ALFORD, GRANVILLE und POMERANCE 1992 bewiesen, dass es unendlich viele CARMICHAEL-Zahlen gibt.

Die kleinste CARMICHAEL-Zahl ist $561 = 3 \cdot 11 \cdot 17$; das folgt leicht aus dem nächsten Satz.

Satz 1 *Eine natürliche Zahl n ist genau dann* CARMICHAEL*-Zahl, wenn sie zuammengesetzt und quadratfrei ist, und $p-1 \mid n-1$ für jeden Primteiler p von n. Eine ungerade* CARMICHAEL*-Zahl hat mindestens 3 Primfaktoren.*

Beweis. „$\Longrightarrow$“: Wäre $p^2 | n$, so enthielte $\mathbb{M}_n$ eine zu $\mathbb{M}_{p^e}$ mit geeignetem $e \geq 2$ isomorphe Untergruppe, also auch eine zyklische Gruppe der Ordnung p; also wäre $p \mid n-1$, Widerspruch. Da aber $\mathbb{M}_n$ eine zyklische Gruppe der Ordnung $p-1$ enthält, gibt es ein Element a der Ordnung $p-1$, und $a^{n-1} \equiv 1 \pmod{n}$, also $p-1 \mid n-1$.

„$\Longleftarrow$“: Da n quadratfrei ist, ist nach dem chinesischen Restsatz die multiplikative Gruppe $\mathbb{M}_n$ das direkte Produkt der zyklischen Gruppen $\mathbb{F}_p^\times$, wobei p die Primteiler von n durchläuft. Da stets $p-1 \mid n-1$, hat jedes Element von $\mathbb{M}_n$ eine Ordnung, die $n-1$ teilt.

Zusatz: Angenommen, $n = pq$ mit zwei Primzahlen p und q, etwa $p < q$. Dann ist $q-1 \mid n-1 = pq-1$, also $p-1 \equiv pq-1 \equiv 0 \pmod{q-1}$, Widerspruch. $\diamond$